

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Ryan S. Burke, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation (“FBI”) and have been so employed since October 2012. I am currently assigned to the FBI’s New Hampshire Resident Agency where I am tasked with investigating violent criminals and major offenders throughout the state. I primarily work alongside the Manchester Police Department (“MPD”) Anti-Crime Unit (“ACU”) as part of an initiative focused on reducing gun violence and other crime in the city of Manchester.

2. Throughout my career, I have led and/or been involved with investigations of robberies, kidnappings, murders, fugitives, extortions, threats, drug distribution, illegal possession of firearms, and other crimes. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses; exploitation of cellular, social media, and Internet Protocol (“IP”) based communications data; execution of search and seizure warrants; wire, electronic, and oral wiretaps; and the execution of arrest warrants.

3. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the violation of various criminal offenses, such as those related to acts of violence, firearms, and controlled substances. For example, I have handled many cooperating sources and witnesses who have provided information to me specifically related to shootings, the distribution of controlled substances, and various firearms offenses. I have also reviewed thousands of court-authorized wiretap intercepts between drug traffickers, violators of firearm offenses, individuals conspiring

to commit armed robberies, and individuals engaged in the violation of other offenses. Many of these investigations have resulted in the execution of search warrants, arrest warrants, and eventual convictions.

4. I submit this affidavit in support of an application for a search warrant pursuant to Federal Rule of Criminal Procedure 41 and Title 18, United States Code, Section 2703(c)(1)(A) to compel Facebook, Inc., 1601 Willow Road, Menlo Park, CA 94025 (“Facebook”) to provide historical and prospective information, further described in Attachment B, for the purpose of locating a “Person to be Arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4), for the following account:

- a. Facebook UID 100004776164012 also known as “timmy.spaulding.73” (“**Target Account**”).

5. Because this warrant seeks the prospective collection of information that may fall within the statutory definitions of information collected by “pen register” and/or “trap and trace device,” *see* 18 U.S.C. §3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. §3123(b)(1).

6. The facts in this affidavit come from my involvement in a collaborative investigation being handled primarily by the FBI and MPD. This affidavit is intended to show there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. On June 28, 2021, the Honorable United States Magistrate Judge Daniel J. Lynch (District of New Hampshire) issued an arrest warrant for Timothy Spaulding (YOB: 1999) for

violations of 21 U.S.C. §§ 846, 841(a)(1), (b)(1)(C) [Conspiracy to distribute and possess with intent to distribute controlled substances], in *United States v. Spaulding, et al.*, 21-mj-171. As such, Spaulding is considered a “Person to be Arrested.”

8. On May 6, 2021, a cellular phone was seized from Spaulding by MPD. It was subsequently examined and imaged pursuant to a search warrant signed by the Judge David A. Anderson (Hillsborough County Superior Court – North). A review of the digital examination suggests Spaulding actively controls and uses the **Target Account**. The review of Spaulding’s phone makes clear that he is an active user of the **Target Account**. Many times a digital examination of a phone will recover only a portion of the data that remains on the device. Even so, hundreds of Facebook Messenger chats exchanged with the **Target Account** were recovered from Spaulding's phone via the examination. Additionally, over 1,000 records related to other Facebook activity from the **Target Account** were recovered, including Check-Ins, Comments, Event Participations, Posts, Reactions, Tags, and Updates. For these reasons, I consider Spaulding to be an active user of the **Target Account** on Facebook.

9. The **Target Account** belongs to Facebook, a free-access social networking website that allows its users to establish accounts through which users can share written news, photographs, videos, and other information with other Facebook users and sometimes with the general public. The **Target Account**, which as of the writing of this affidavit appears to be active, also clearly and publicly displays photographs of Spaulding. Consequently, I believe the **Target Account** belongs to, is controlled by, and utilized by Spaulding.

10. Based on my training, experience, and discussions with other law enforcement officers and Facebook representatives, I know the following about Facebook:

- a. Facebook asks users to provide basic contact information, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, tokens, and other personal identifiers;
- b. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information in the user's account available only to himself or herself, to other specified Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users;
- c. Facebook accounts include privacy settings that users can adjust and control. Depending on the user's privacy settings, Facebook may also obtain and store the physical location, or GPS data, of the user's device(s) as they interact with the Facebook service on those device(s);
- d. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile; and
- e. Facebook retains IP address logs for a given user ID. These logs may contain information about the actions taken by the user ID on Facebook, including

information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

11. Therefore, the computers of Facebook are likely to contain all the material listed above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, location/GPS information, IP address logs, and account details. Some of the information, such as location/GPS information and IP address logs, can be prospectively provided by Facebook.

12. The information in Facebook's possession is critical for law enforcement in their efforts to locate Spaulding and effect his arrest warrant as Spaulding has recently been cycling phone numbers in an effort to evade capture. In particular, the subscriber information for the **Target Account** may include Spaulding's active phone number and email address, both of which could be further exploited to locate and arrest him. His recent messaging content may reveal his current whereabouts as he actively avoids law enforcement. The prospective data will allow law enforcement to monitor his Facebook activity in real-time: the location/GPS data could immediately identify Spaulding's location, while the IP address logs could be further exploited to identify his location.

13. I request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate Spaulding outside of daytime hours.

14. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant authorizing the use of a CSS to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate

notice to the subscribers or users of the Target Phones would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to change patterns of behavior, notify confederates, and/or flee from prosecution. See 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. See 18 U.S.C. § 3103a(b)(2).

CONCLUSION

15. Based on the information described above, I have probable cause to believe that Spaulding owns and controls the **Target Account** and that the information in Facebook's possession will aid law enforcement in locating Spaulding, a "Person to be Arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

/s/ Ryan S. Burke
Ryan S. Burke, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: **Jul 9, 2021**

Time: 5:01 PM, Jul 9, 2021

Andrea K. Johnstone



The Honorable Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A

This search warrant is being sought for the data specified in Attachment B for the following Facebook account, which is hosted by Facebook, Inc. 1601 Willow Road, Menlo Park, CA 94025: Facebook UID 100004776164012 also known as “timmy.spaulding.73”

ATTACHMENT B

I. Historical Information to be Disclosed by Facebook, Inc. (“Facebook”)

Facebook is required to disclose the following information to the government for the User ID listed in Attachment A for the time period of July 1, 2021 to present:

- a. Extended subscriber information for the account, including but not limited to the user’s full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, tokens, and other personal identifiers;
- b. All location information; GPS data; and IP addresses for log-ins/log-outs/intra-session messaging, posts, and other activity; and
- c. Facebook messenger content, including but not limited to dates, times, content, and conversation participant UIDs.

II. Prospective Information to be Disclosed by Facebook, Inc. (“Facebook”)

Facebook is required to disclose the following information to the government for the User ID listed in Attachment A for forty-five (45) days beginning on the date of installation:

- a. All physical location data, to include GPS and IP address information, collected by Facebook for the user of the account, including any data collected by Facebook’s location services via the user’s mobile phone or other device, on a real-time or near-real time basis; and
- b. Because this warrant is designed to comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127, all dialing, routing, addressing, and signaling information associated with each communication to or from the **Target Account**, including (a) the headers of messages, including the source and destination addresses of all messages directed to or originating

from the **Target Account** along with the routing information, IP addresses for log-ins/log-outs and intra-session IP addresses associated with messages and all other activity, dates, times, and sizes of such messages and the number and size of any attachments, but not content located in headers, such as subject lines, on a real-time or near-real time basis.

III. Information to be Seized by the Government

All data disclosed by Facebook pursuant to this attachment. This data shall be made accessible by Facebook to the Federal Bureau of Investigation 24/7, day or night, and emailed to Special Agent Ryan S. Burke at rsburke@fbi.gov at regular intervals.

IV. Time for Production by Facebook and Duration

Facebook shall begin producing the information required by this attachment no later than five (5) days of the date of service of this warrant and for a period of forty-five (45) days from the initial date of production.